REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 03-05-2010	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE NO AIR: CYBER DEPENDENCY AND THE DOCTRINE GAP	**5a. CONTRACT NUMBER**
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) DAVID A. RICKARDS, Maj, USAF	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	**10. SPONSOR/MONITOR'S ACRONYM(S)**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Despite concerted efforts to defend them, military cyber networks remain vulnerable to attack. For the U.S. military to maintain operational agility, operational doctrine should expand to include methods designed to ensure unhindered operations in a degraded cyber environment. The need for expansion in cyber doctrine stems from four areas: the nature of the cyberspace domain, the military's growing dependency on it, the threat environment, and doctrinal gaps. At the operational level, shortcomings in doctrine affect training, planning, and the U.S. military's ability to seize and maintain the initiative. Because of current inabilities to protect much of its cyber network from attack, U.S. military dependency on the cyber domain becomes a critical vulnerability for an enemy to exploit. By training like it expects to fight, ensuring operational planning assumptions are accurate, and emphasizing decentralized execution of commander's intent, the U.S. military can better operate in a challenged or austere cyber network environment.

15. SUBJECT TERMS
cyber, C2, dependency, vulnerable, doctrine, initiative, degraded, network, attack, environment

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		22	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3414

NAVAL WAR COLLEGE
Newport, R.I.

NO AIR: CYBER DEPENDENCY AND THE DOCTRINE GAP

by

David A. Rickards

Major, USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _________________________

3 May 2010

Abstract

Despite concerted efforts to defend them, military cyber networks remain vulnerable to attack. For the U.S. military to preserve its operational agility, operational doctrine should expand to include methods designed to ensure unhindered operations in a degraded cyber environment. The need for expansion in cyber doctrine stems from four areas: the nature of the cyberspace domain, the military's growing dependency on it, the threat environment, and doctrinal gaps. At the operational level, shortcomings in doctrine affect training, planning, and the U.S. military's ability to seize and maintain the initiative. Because of current inabilities to protect much of its cyber network from attack, U.S. military dependency on the cyber domain may become a critical vulnerability for an enemy to exploit. By training like it expects to fight, ensuring operational planning assumptions are accurate, and emphasizing decentralized execution of commander's intent, the U.S. military can better operate in a challenged or austere cyber network environment.

INTRODUCTION

We cannot hide behind the Maginot line of network security.
—Admiral Stavridis

In 2007, network intruders, ostensibly from China, infiltrated the data files of defense contractors developing the Joint Strike Fighter, making off with sensitive design plans and defense technology.[1] In the summer of 2009, North Korean computer hackers penetrated cyber security defenses in South Korea, broke into computers and "acquired copies of plans spelling out how the United States and South Korea would respond if the North attacked the South."[2] Most recently, Iraqi insurgents used inexpensive, commercially available tools to monitor video feeds from U.S. unmanned aerial vehicles.[3] These are just a few of the many recent examples that show the vulnerability of cyber networks to attack. The United States military, in particular, has taken notice, investing heavily in cyber network defense and expanding into offensive techniques designed to preserve its critical cyber capabilities.

Despite these efforts, a gap remains. Between the poles of cyber offense and defense lies a no-man's land of contested territory. In this gray area, no doctrinal foundation exists to guide the 21st-century American warrior through the fog and friction of degraded cyber network operations. Two things remain constant for the near future: the likelihood that combat operations will take place in a contested cyber environment, and the U.S. military's dependence on the cyber domain as a key enabler for network-centric operations. Given this, our approach to war must change at a foundational, doctrinal level. For the U.S. military to

[1] Siobhan Gorman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter Jet Project," *Wall Street Journal*, 21 April 2009, http://online.wsj.com/article/SB124027491029837401.html#articleTabs%3Darticle (accessed 16 April 2010).
[2] William Mat, "In Cyber War, Most of U.S. Must Defend Itself," *Defense News*, 1 February 2010, 29.
[3] Ibid.

preserve its operational agility, operational doctrine should expand to include methods designed to ensure unhindered operations in a degraded cyber environment.

BACKGROUND

The U.S. military is only beginning to wrap its doctrinal arms around the best approach to cyber war. As Mike McConnell states, national security policy has "yet to address the most basic questions about cyber-conflicts."[4] The absence of adequate doctrine to cover operations in cyberspace is natural and expected, for doctrine grows from lessons learned and experience on the battlefield—experience the military is still gathering and assessing. The need for expansion in U.S. military cyber doctrine stems from four areas: the nature of the cyberspace domain, the growing dependency on it, the threat environment, and gaps in doctrine.

The National Military Strategy for Cyberspace defines cyberspace as "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange information via networked systems and physical infrastructures."[5] Unlike the domains of air, sea, and space, cyberspace has no set dimensions. Though cyberspace depends on physical infrastructure (servers, satellites, undersea cables, fiber optic lines, etc.), it is ultimately an ethereal domain, comprising mere ones and zeros. Cyberspace can't be controlled in the same way one can gain sea control or air superiority. It is "a domain in which both friendly and enemy forces have ability to achieve equal access."[6] Cyberspace

[4] Mike McConnell, "Mike McConnell on How to Win the Cyber-War We're Losing," *Washington Post*, 28 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (accessed 28 February 2010).
[5] U.S. Department of Defense, *The National Military Strategy for Cyberspace Operations (U)* (Washington, DC: 2006), ix.
[6] Richard M. Crowell, War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare (Newport, RI: Naval War College, 2009), 8.

operates in and through the other four spatial domains, from land-based servers and cell phone towers, to air-based surveillance platforms and transmission nodes, sea-based ships and radar, and space-based satellites.[7]

The Department of Defense (DOD) footprint in cyberspace is quite large. The DOD uses over 3.5 million computers on some 10,000 local area networks located on 1,500 bases in 65 countries.[8] These computers are connected by 120,000 circuits supporting 35 major network systems over three router-based architectures.[9] Over the last few decades, technology advances have gradually integrated computers into every aspect of U.S. weapon systems; as a result, the U.S. military has come to rely heavily on cyber networks. Richard Crowell, in his primer on war in the information age, expounds on the dependence of modern militaries on cyber network capabilities:

> Many militaries now rely almost exclusively on cyberspace to move information to decision makers--commanders and troops. Military uses of cyberspace include e-mail (unclassified and classified), chat (in various commercial formats), Video Teleconference (VTC), Global Command and Control System (GCCS), Global Transportation Network (GTN), In-Transit Visibility (ITV), Joint Tactical Radio System (JTRS), Blue Force Tracker (BFT), Theater Battle Management Control System (TBMCS), Link 11 and Link 16 Data Link Systems, Unmanned Aerial Systems (UAS, i.e. Global Hawk and Predator), Global Positioning System (GPS), and Joint Direct Attack Munitions (JDAM).[10]

This is not an exhaustive list, and it is constrained to cyber capabilities the military owns and operates. Yet the greater part of cyber infrastructure, over 90%, is found in the relatively

[7] Crowell, 21.
[8] Elihu Zimet and Charles L. Barry, "Military Service Overview," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles: Potomac Books, Inc., 2009), 294.
[9] Ibid.
[10] Crowell, 6.

unprotected civilian sector.[11] The U.S. military requires constant access to the "global communications backbone" and uses networks that "rely on commercial connectivity;" this open infrastructure provides functionality for unclassified cyber networks as well as for secure, controlled systems (e.g., the Secret Internet Protocol Router Network, Secure Telephone Units).[12]

Our military's dependence on cyber technology is both a blessing and a curse, for as Kamal Jabbour states, it creates "a dichotomy of net-centric military superiority and a commensurate reliance on vulnerable technology."[13] The vulnerability he speaks of is partly due to budget constraints: in time of war, cash-strapped acquisition structures in the Defense Department have gradually migrated away from expensive, stand-alone systems towards commercial off-the-shelf alternatives that are less costly and faster to field.[14] Unfortunately, what the system gained in money and time has been offset to some extent by losses in the area of cyber security, because commercial systems often aren't designed to operate in a threat environment.

This development comes at a time when many nations are heavily investing in capabilities designed to take down military cyber networks. Russia, in operations against Georgia in 2008, demonstrated considerable prowess in computer network attack.[15] China is preparing for a wartime scenario of attacking what they see as a "soft underbelly," a modern

[11] U.S. Air Force Space Command, *The United States Air Force Blueprint for Cyberspace* (Colorado Springs, CO: 2 November 2009), 6.
[12] Zimet and Barry, 287.
[13] Kamal Jabbour, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly,* Spring 2010, 63.
[14] Ibid., 64.
[15] Eric D. Trias and Bryan M. Bell, "Cyber This, Cyber That . . . So What?" *Air & Space Power Journal*, Spring 2010, 90-100.

military's dependence on computer networking.[16] Indeed, one of the fastest growing subjects in the People's Liberation Army research literature is "defending and attacking computer networks."[17] According to Crowell, "There have been innumerable Chinese military strategy books written on cyberspace operations, information warfare, information operations, and electronic warfare."[18] In one of those works, two Chinese general officers plainly stated their nation's goal as being "proficient at using electronic feints, electronic camouflage, electronic jamming, virus attacks, and space satellite jamming and deception, leading the enemy to draw the wrong conclusion and attaining the goal of strategic deception."[19] Other states known for their investment in cyber exploitation techniques are Israel, France, and Brazil.[20]

Given the nature of cyberspace, the U.S. military's dependence upon it, and the growing threat, joint doctrine should provide a firm foundation for operating in such a vital domain as cyberspace. Yet joint doctrine doesn't discuss cyberspace in a separate and distinct manner. Instead, it incorporates cyberspace operations across multiple disciplines and operational areas. The biggest of these is Information Operations (Joint Pub 3-13). According to Information Operations (IO) doctrine, Computer Network Operations comprise computer network attack, computer network defense, and related computer network exploitation operations (sometimes called enabling or support operations).[21] Besides IO, one can also find cyber-related doctrine in directives related to intelligence, communications, command and control, electronic warfare, and information management. Service doctrines take their

[16] James Fallows, "Cyber Warriors," *The Atlantic Monthly*, Vol. 305, No. 2, March 2010, 63.
[17] Ibid., 63.
[18] Crowell, 8.
[19] Peng Guangqian and Yao Youzhi, ed., *The Science of Military Strategy* (Beijing, People's Republic of China: Military Science Publishing House, 2005), 475-476.
[20] Fallows, 62.
[21] Chairman, U.S. Joint Chiefs of Staff, *Information Operations*, Joint Publication (JP) 3-13 (Washington, DC: CJCS, 13 February 2006), II-5.

cue from joint and DOD publications. All have the same architecture: attack, defense, and exploitation/support. Only if one expands the search to national-level documents can one find language condoning the “ability to operate through degradation.”[22] See Appendix A for a brief compendium of joint and service doctrine addressing cyberspace.

When it comes to the cyber domain, joint doctrine is lacking because it mistakenly takes the same approach as with any other realm: defend the domain, attack through the domain, and exploit the domain to support further joint operations. This approach is flawed because there is no recognition of the unique characteristics that make cyberspace fundamentally different from the other domains. Cyberspace should not be approached in the same manner as air, land, sea, and space.

In the four physical domains, a military fights for control over—and exploitation of—disputed territory. A military uses airpower, for example, to ward off enemy aircraft and suppress enemy air defenses, all with the goal of controlling and exploiting the air for military purposes. A naval power fights to control the sea so they may use it for desired ends and objectives, at times denying similar use to an enemy. With cyberspace, the same approach is anathema. A military force may use cyber power to command forces, operate weapon systems, and confuse the enemy, but in cyberspace, “control” of the domain becomes a misnomer. In a 2009 RAND report, Martin Libicki reached the same conclusion: “The question of cybersupremacy is meaningless and, as such, is not a proper goal for operational cyberwarriors . . . because cyberspace is not a unitary domain. (Opposing) organizations can

[22] U.S. Department of Defense, *The National Military Strategy for Cyberspace Operations (U)*, 10-11.

simultaneously keep each other off their own networks."[23] Cyberspace is radically different from other domains because a capable enemy can alter the medium itself. This basic difference makes the cyber domain stand out in sharp contrast to other warfighting domains, and it means a fundamental shift in the way one approaches cyberspace doctrinally. Unfortunately, current doctrine remains wedded to the "attack, defend, exploit" mantra that works well only for spatially oriented (i.e., unitary) domains.

DISCUSSION

The U.S. military has a doctrine gap: joint operational doctrine does not adequately address operations in a degraded cyber network environment. At the operational level, paucity of doctrine affects training, planning, and our ability to seize and maintain the initiative.

First, the gap in cyber doctrine affects operational training. Military readiness comes, in large part, from training and preparation. "Train like you fight" is an often quoted military adage built on lessons learned. If a military force doesn't accurately prepare for war during times of peace (or if it practices the wrong things), it will learn hard lessons when the real fighting starts. Failing to train for operations in a degraded cyber environment will lead to lower operational readiness levels, simply because commanders and the forces they lead will have no practical experience fighting under such conditions. In a recent address to students at the Naval War College, the Commander, U.S. Joint Forces Command, lamented the military's lack of experience with operations in a degraded communications environment:

[23] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 141.

"We used to practice comm out procedures in the Cold War. How many times have we practiced them since?"[24]

Doctrine and training go hand in hand. As military theorist Dr. Milan Vego states, doctrine and training "are interrelated and affect each other in many ways. A force can be numerically larger and excellently armed and equipped but still be ineffective because of severe training deficiencies."[25] Doctrine, and the training inspired by it, is influenced by experience gained on the battlefield. Recent experience, however, should not be seen as adequate feedback in this regard, because the U.S. military has yet to face a true cyber competitor in war. Our cyber-enabled approach to operations has not been seriously contested in either Afghanistan or Iraq. This points to a problem, for as Vego relates, "Suitable doctrine for . . . untested technologies must be subjected to series of stringent tests under realistic conditions of the modern battlefield."[26]

Gaps in doctrine can sometimes be ameliorated through a particular type of training: the war game. As Admiral Nimitz said recalling the benefits of his time spent wargaming at the Naval War College, nothing surprised him in WWII: "The war with Japan had been (enacted) in the game room here by so many people in so many different ways that nothing that happened during the war was a surprise. Absolutely nothing except the Kamikaze."[27] But as Nimitz implies, war games must be open to innovative (and unpopular) inputs from

[24] Gen James N. Mattis, Commander, U.S. Joint Forces Command (speech, Naval War College, Newport, RI, 25 March 2010).
[25] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: Naval War College, 2009), III-45.
[26] Ibid., IX-10.
[27] Matthew Caffrey, "Toward a History Based Doctrine for Wargaming," *Air and Space Power Journal*, April 2000, 33-56.

both sides or "the lessons learned . . . are essentially useless as the basis for doctrine."[28] War games with degraded cyber environments may not be popular, easy, or allow us to exercise our full military might, but they are vital inputs for building a realistic and robust doctrine for cyberspace operations.

Second, shortfalls in cyber doctrine have negative effects on operational planning, especially in the area of assumptions. Historically, military planners have had difficulty making accurate assumptions about enemy behavior in "new" domains. The undersea environment is one example. German use of submarines to conduct *guerre de course* in World War I was not predicted or expected by Great Britain or the United States. Many naval planners assumed no one would adopt such a "barbaric" approach to war. That assumption was based on a doctrine which made no allowance for enemy employment of submarines to attack sea commerce, much less how to protect commercial vessels from undersea attack. In the air domain, consider the Japanese use of the kamikaze pilot. The U.S. Navy in World War II had limited defenses against determined suicide attacks. Again, doctrinal blind spots led to inaccurate operational assumptions.

In the cyber domain, inadequate doctrine may again lead to poor planning assumptions. In fact, faulty assumptions are *already* resident in doctrine, for current doctrine assumes the cyber domain will be available for attack, defense and exploitation. Here, comparing the cyber domain to the air domain is helpful. Air forces have as a basic assumption that the earth will remain covered in an atmosphere for the foreseeable future (i.e., there will be air to fly in). Stating this assumption seems absurd, but only because the air domain is physical.

[28] Vego, XII-8.

When translated to the cyber domain the comparison becomes relevant, for in cyberspace the assumption of domain presence must be made anew each time a cyber sortie is conducted.

A new logic is required, because "cyberspace is so different a medium. The concepts of deterrence and war . . . lack the logical foundations that they have in the nuclear and conventional realms."[29] In cyberspace, a capable enemy may be able to negate or degrade the domain itself. This means the first thing the operational commander may have to determine is the current state of the cyber environment. "While traditional domains are fixed in size—the amount of available land, sea, air, and orbital space is essentially constant—the cyberspace domain changes dynamically and increases indefinitely in size and shape."[30] Despite current doctrine's unwritten assumption to the contrary, the operational commander cannot trust in the constant availability of the cyber domain for operations.

There is a third consequence of inadequate cyber doctrine. Along with training and planning, gaps in doctrine affect the U.S. military's ability to seize and maintain the operational initiative. In a degraded cyber environment, the United States may find itself devolving to slower, non-networked methods of operational command and control. Sudden communications parity with the enemy (or even worse, sub-parity) would seriously slow our operational tempo and make the initiative—something we've been used to possessing from H-hour—less a thing to be seized and more an object to chase after. Missions dependent on cyber connectivity would have to be retooled before execution.

Keeping the operational initiative in a cyber degraded environment is only viable if local commanders retain the ability to assure the mission. Kamal Jabbour explains why this is so: "Cyberspace play(s) the dual role of communicating situational awareness to commanders

[29] Libicki, 5.

[30] Jabbour, 66.

and carrying back command and control instructions representing their intent. Under no circumstance can the responsibility for mission assurance shift away from the mission command to a JFC [Joint Force Commander] responsible for securing the network."[31] In other words, building mission dependencies into a deniable cyber network is problematic unless local commanders retain the ability to innovate, find work arounds, and meet mission objectives. If, as General Mattis says, "We are going to have to fight without communications," seizing the operational initiative cannot be dependent on cyber network availability.[32] In that light, a cyber doctrine that presumes network availability has limited utility.

By way of counterargument, some cyber experts believe our current approach to doctrine is adequate and sufficient. For them, an attack on U.S. military computer networks would "offer only temporary disruption," causing major upheaval but only minor long-term effects.[33] Hopefully this is true, but its very admission betrays a willingness to cede the initiative to the enemy. While one recovers from the "temporary disruption" allowed above, an enemy looking to capitalize on opportunity may conduct strikes with more enduring effects. Doctrine should posture the U.S. military for success through disruption, however fleeting it may be, and not forfeit ground to prospective cyber enemies so easily.

Other authorities believe the United States is attributing hostility where none exists, including the White House Cybersecurity Coordinator, Howard Schmidt. In an attempt to calm fears over malicious code and malevolent hackers, Schmidt reframed the situation by

[31] Jabbour, 68.
[32] Mattis, 25 March 2010.
[33] Libicki, 153.

saying, “There is no cyberwar.”[34] Some scholars have added to Schmidt’s chorus by citing benign intent. One Chinese graduate student who recently published a paper on “how to attack a small U.S. power grid sub-network in a way that would cause a cascading failure,” said his research wasn’t malicious; instead, he was merely pursuing a legitimate “technical exercise” aimed at uncovering ways to protect civilian infrastructure.[35] The U.S. military, however, isn’t charged with defending America against *intentions* but rather against *capabilities*. It is the potential threat one hedges against.

Still others contend the very nature of the Internet provides all the mission security a modern military needs. Decentralization and packet routing make it impossible to “stop” the Internet from working, as there are numerous routes to reach the same destination. This argument ignores the fact that, at some point in its journey, the majority of Internet traffic routes through important nodes—decisive points that can greatly affect the flow of information.[36] As Vego reminds us, “one or more (command, control, communication, and computer) nodes may be of such critical importance that their destruction immediately degrades the functioning of the entire system.”[37] But this contention also errs in scope, focusing as it does on tactical fixes to operational problems. Our present course will win “only so long as (we) do not face peer competitors who achieve superiority not through the

[34] Ryan Singel, “White House Cyber Czar: ‘There Is No Cyberwar,’” *Wired.com*, 4 March 2010, http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ (accessed 5 March 2010).

[35] John Markoff and David Barboza, “Academic Paper in China Sets Off Alarms in U.S.,” *New York Times*, 20 March 2010, sec. 1, p. 11.

[36] John Markoff, “Scientists Strive to Map the Shape-Shifting Net,” *New York Times*, 1 March 2010, http://www.nytimes/com/2010/03/02/science/02topo.html (accessed 13 March 10).

[37] Vego, VIII-49.

number of platforms and advanced weapons but by thinking and acting operationally instead of tactically."[38]

CONCLUSIONS

Given our doctrinal shortcomings regarding cyberspace operations, one can conclude the U.S. military has cause for concern when it comes to its ability to operate in a degraded cyber environment. For us, the consequences of an enemy cyber attack are directly related to our dependence upon the cyber domain. Without a way to break our fall, cyber dependency becomes a critical vulnerability for an enemy to exploit.

Dr. Vego has much to say on this point: "If (a military) relies extensively on computerized systems for command and control, intelligence, ballistic missile defense or theaterwide air defenses, it is possible to indirectly attack the (military's) center of gravity through an attack against (its) cybernetic-oriented decisive points."[39] To borrow language from joint doctrine, the U.S. military has a critical requirement for cyber networks; the cyber domain is an essential resource for our operational approach to war. That critical requirement, benign in itself, becomes a critical vulnerability because it is susceptible to "direct or indirect attacks" which could create "decisive or significant effects."[40]

Our doctrinal gap makes us vulnerable to exploitation. We are organized to attack (offensive operations) and defend (defensive operations), but we aren't doctrinally prepared to operate in the middle—the area in between that exists when our attacks don't completely negate the enemy threat and our defenses repel some (but not all) of it. Joint doctrine doesn't

[38] Milan N. Vego, *Major Naval Operations*, Newport Papers no. 32 (Newport, RI: Naval War College Press, 2008), 21.
[39] Vego, *Joint Operational Warfare*, IX-111.
[40] Chairman, U.S. Joint Chiefs of Staff, *Joint Operational Planning*, Joint Publication (JP) 5-0 (Washington, DC: CJCS, 26 December 2006), IV-11.

provide for operations through the fog and friction caused by cyber attack, it merely assumes we can assail the problem and negate it, or defend against it so thoroughly it ceases to be an issue.

Unfortunately, this all-or-nothing approach does not agree with the lessons of history. Examining recent examples of conflicts where the cyber domain was used as a means to affect operations can be a profitable exercise, with doctrinal implications. Russia's alleged used of denial of service attacks against Estonia and Georgia in 2007 and 2008 are well known and should be studied for lessons applicable to operational doctrine.[41] Another opportunity to observe lessons occurred in the summer of 2006, when Israel found itself fighting a Hezbollah enemy that had matured well beyond its days of guerilla tactics. Hezbollah used their knowledge of Israeli cyber networks to intercept Israeli Defense Force cell phone calls as well as "U.S.-made single channel ground and airborne radio system (SINCGARS) frequency hopping combat radio transmissions."[42] Israel's vulnerability to cyber attack was telling. Though the extent to which their operational doctrine left them unable to operate in a degraded cyber environment is beyond the scope of this paper, the fact they had trouble at all has obvious implications.

RECOMMENDATIONS

A new way of operational thinking is required, one that allows us to cope with "decision cycles (that) hover around a fraction of a second."[43] Doctrine must adjust to the realities of the cyber domain and equip our military with a firm foundation for fighting in a degraded cyber environment. The U.S military should train like it expects to fight, ensure operational

[41] Mat, 30.
[42] Crowell, 11.
[43] Jabbour, 66.

plans account for network degradation, and emphasize decentralized execution of commander's intent.

Train like you expect to fight. The U.S. military should regularly train in cyber-degraded conditions until operating in such an environment becomes second nature. The ubiquity and dependability of computer networks should be periodically challenged to see if operational agility remains. Regular forces should learn to operate without a communications tether to higher headquarters, a notion advocated by General Mattis during his recent visit.[44] Operational command and control nodes should adopt procedures which allow us to keep our momentum despite operating in a degraded cyber network. War games should drive out the unseen consequences of degraded cyber networks. Once the above actions are taken, sound doctrine can be written to capture the lessons learned and to guide the future application of combat power.[45]

Ensure operational plans include provisions for cyber network degradation. Operational planners should build branches and sequels into operational plans that take into account the real potential for adversary actions against our cyber network. Estimates of enemy cyber warfare capabilities should be realistic, and consequences of enemy cyber actions should be based on accurate doctrine regarding the nature of the cyber domain. If an operational commander believes an adversary can degrade or deny access to friendly cyber assets, it follows he or she should plan to fight without the aid of reliable information.[46]

Emphasize decentralized execution. Commanders should adopt command and control methods designed to ensure uninterrupted operations in a degraded cyber environment. By

[44] Mattis, 25 March 2010.
[45] Vego, *Joint Operational Warfare*, XII-3.
[46] Crowell, 24.

doing so, an operational commander will better preserve the initiative and improve his chances to "fight through" the fog of war. Operational commanders should consider questions posed by Crowell: "How do plans and orders move up and down the chain of command when the electromagnetic spectrum is disturbed or denied? In a disrupted or denied electromagnetic environment can the operational commander communicate with his subordinates and superiors?"[47] Decentralized execution techniques offer a ready solution and should be adopted upon the first hint of cyber domain degradation. In this way, dependence on communications will be reduced, reaction time will be shortened, and, "in the case of . . . a total breakdown of communications, lower-echelon commands (will be) better prepared to act on their own initiative."[48]

As the Joint Operating Environment 2010 states, "many (advances in communication and information technologies) will be available to America's opponents. It is . . . essential that the Joint Force be capable of functioning in a hostile information environment, so as not to create an Achilles' heel by becoming too network dependent."[49] In future wars, the opponent better able to operate in a degraded cyber environment will be the one who can seize the operational initiative and carry the field. The U.S. military should take a hard look at its ability to operate with "no air"—without the full use of the cyber domain. To preserve our operational agility, operational doctrine should expand to include methods designed to ensure unhindered operations in a degraded cyber environment.

[47] Crowell, 21.

[48] Vego, *Joint Operational Warfare*, VIII-9.

[49] U.S. Joint Forces Command, *Joint Operating Environment 2010* (Suffolk, VA: 18 February 2010), 34.

APPENDIX A

U.S. Military Doctrine on Cyberspace and Network Warfare (not exhaustive)

Joint Resources

- DOD Information Operations Roadmap, created in 2003, declassified Jan 2006
- Joint Information Operations Planning Handbook - Joint Command, Control and Information Warfare School - Joint Forces Staff College
- JP 3-13, Information Operations
- JP 3-13.1, Electronic Warfare
- DOD Directive 3222.4, "Electronic Warfare (EW) and Command and Control Warfare (C2W) Countermeasures"
- DOD Directive O-3600.1, "Information Operations"
- DOD Directive O-8530.1, "Computer Network Defense (CND)"
- DOD Instruction 3608.11, "Information Operations Career Force"
- DOD Instruction 3608.12, "Joint Information Operations (IO) Education"
- CJCSM 3320.01A, Joint Operations in the Electromagnetic Battle Space

Army Resources

- FM 3-13, Information Operations - Doctrine, Tactics, Techniques, and Procedures
- FM 2-0, Intelligence and Electronic Warfare Operations
- FM 3-36, Electronic Warfare in Operations
- FM-34-37, Strategic, Departmental, and Operational Intelligence and Electronic Warfare (IEW) Operations
- FM 90-2, Battlefield Deception

Navy & Marine Resources

- OPNAVINST 3430.25 Information Warfare and Command and Control Warfare
- Naval Doctrine Publication 6 - Naval Command and Control
- MCDP 6 Command and Control
- A Concept for Information Operations, USMC

Air Force Resources

- AFI 10-703 Electronic Warfare Integrated Reprogramming
- AFI 10-706 Electronic Warfare (EW) Operations
- AFI 33-115, vol. 3, Air Force Network Operating Instructions
- AFDD 2-5 Information Operations
- AFDD 2-5.1 Electronic Warfare Operations
- AFDD 2-9 Intelligence, Surveillance, and Reconnaissance Operations

SELECTED BIBLIOGRAPHY

Alberts, David S. and Richard E. Hayes. *Power to the Edge: Command . . . Control . . . in the Information Age*. Washington, DC: DOD Command and Control Research Program, 2005.

U.S. Air Force Space Command. *The United States Air Force Blueprint for Cyberspace*. Colorado Springs, CO: 2 November 2009.

Caffrey, Matthew. "Toward a History Based Doctrine for Wargaming." *Air and Space Power Journal*, Fall 2000, 33-56.

Crowell, Richard M. *War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare*. Newport, RI: Naval War College, 2009.

Fallows, James. "Cyber Warriors." *The Atlantic Monthly*, Vol. 305, No. 2, March 2010, 58-63.

Gompert, David C., Irving Lachow, and Justin Perkins. *Gaining Cognitive Advantage in Networked Warfare*. Washington, DC: National Defense University, 2005.

Gorman, Siobhan, August Cole, and Yochi Dreazen. "Computer Spies Breach Fighter Jet Project." *Wall Street Journal*, 21 April 2009, http://online.wsj.com/article/SB124027491029837401.html#articleTabs%3Darticle (accessed 16 April 2010).

Guangqian, Peng and Yao Youzhi, ed. *The Science of Military Strategy*. Beijing, People's Republic of China: Military Science Publishing House, 2005.

Heickerö, Roland. "Thoughts on the Application of Military Theory to Information Operations and Network Centric Warfare." *IO Sphere*, Fall 2005, 24-26.

Jabbour, Kamal. "Cyber Vision and Cyber Force Development." *Strategic Studies Quarterly*, Spring 2010, 63-73.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND, 2009.

Magnuson, Stew. "Cyber-Attack." *National Defense*, Vol. 93, Iss. 668, July 2009, 22.

Maiers, Mark W. and Timothy L. Rahn. "Information Operations and Millennium Challenge." *Joint Forces Quarterly*, Vol. 35, October 2004, 83-87.

Markoff, John. "Scientists Strive to Map the Shape-Shifting Net." *New York Times*. 1 March 2010. http://www.nytimes/com/2010/03/02/science/02topo.html (accessed 13 Mar 10).

Mat, William. "In Cyber War, Most of U.S. Must Defend Itself." *Defense News,* 1 February 2010, 29.

Mattis, Gen James N. Speech. Naval War College, Newport, RI, 25 March 2010. (attribution authorized per e-mail, 31 March 2010).

McConnell, Mike. "Mike McConnell on How to Win the Cyber-War We're Losing." *Washington Post,* 28 February 2010. http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html (accessed 28 February 2010).

Singel, Ryan. "Cyberwar Hype Intended to Destroy the Open Internet," *Wired.com*, 1 March 2010. http://www.wired.com/threatlevel/2010/03/cyber-war-hype/ (accessed 4 March 2010).

______. "White House Cyber Czar: 'There Is No Cyberwar.'" *Wired.com*, 4 March 2010. http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar/ (accessed 5 March 2010).

Stavridis, ADM James G., Supreme Allied Commander, Europe. Address. Armed Forces Communications and Electronics Association, San Diego, CA, 2 February 2010.

Trias, Eric D. and Bryan M. Bell. "Cyber This, Cyber That . . . So What?" *Air & Space Power Journal,* Spring 2010, 90-100.

"U.S. Army Completes Field Testing of Next-Gen FBCB2 Software." *Globe Newswire,* 25 February 2010. http://www.deagel.com/news/US-Army-Completes-Field-Testing-of-Next-Generation-FBCB2-Software_n000007132.aspx (accessed 26 February 2010).

U.S. Department of Defense. *The National Military Strategy for Cyberspace Operations (U).* Washington, DC: DOD, 2006.

U.S. Joint Forces Command. *Joint Operating Environment 2010*. Suffolk, VA: 18 February 2010.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. Joint Publication (JP) 3-13, Washington, DC: CJCS, 13 February 2006.

______. *Joint Operational Planning*. JP 5-0. Washington, DC: CJCS, 26 December 2006.

Vego, Milan, N. *Joint Operational Warfare: Theory and Practice*. Newport, RI: Naval War College, 2009.

______. *Major Naval Operations*. Newport Papers, no. 32. Newport, RI: Naval War College Press, 2008.

Walker, James D. "Weapon System Effectiveness." *Aerospace America*, Vol. 47, December 2009, 62.

Zimet, Elihu and Charles L. Barry. "Military Service Overview." In *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Dulles: Potomac Books, Inc., 2009.